Federal Electronic Government Infrastructure
The E-Authentication Gateway – Connecting People to Services

Background:

Public trust in the security of the information exchanged over the Internet will play a vital role in an electronic Government transformation. The Government must address the issues of user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary. Thus, solutions that provide this type of protection are critical components of an organization's cyber security profile.

The current administration, recognizing the need for identity authentication to implement an E-government, initiated the E-Authentication Initiative. Common authentication services for use across government agencies will reduce the burden on the public and better leverage the government's investments.

Purpose:

This paper presents key concepts, policy and design issues and needs associated with the deployment of a Federal E-Authentication Gateway. The paper contains an overview of the authentication infrastructure that is critical to achieve the President's Management Agenda for E-Government. This paper also presents the proposed operational concept of the Gateway and its core requirements. This public document is intended as input and support in assisting the Federal Government in establishing a design that fits within the Federal enterprise architecture framework, testing, and evaluation for ongoing E-Government authentication and identity management needs.

Overview of the Authentication Gateway:

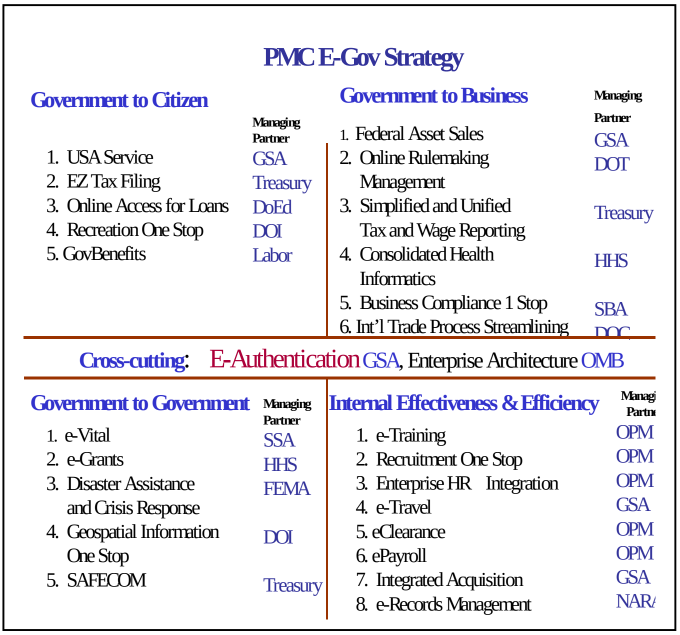
President's Management Agenda

- ***1st Priority: Make Government citizen-centered.***
- **5 Key Government-wide Initiatives**:
  - Strategic Management of Human Capital
  - Competitive Sourcing
  - Improved Financial performance
  - *Expanded Electronic Government*
  - Budget and Performance Integration

Expanding E-Government to enhance citizen-centric government services is a key initiative of the President's domestic management agenda. To advance this agenda, the Administration established the E-Gov Task Force in July 2001 under the Office of Management and Budget (OMB). The Task Force identified the key E-Government initiatives across the Federal Government best positioned to support the management agenda. The President's Management Council approved 24 initiatives in November 2001. These 24 initiatives defined government services and business transactions within four segments: citizen, business, government, and internal operations. All of the initiatives represent cross-agency efforts and are targeted for implementation within 18 – 24 months. In addition, all require some degree of authentication to support some or all of the business services and transactions. It is recognized that the four segments have different characteristics, and thus different authentication requirements.

To support the needs of all of the initiatives, the e-Authentication Integrated Project Team, managed by the General Services Administration was directed to provide common authentication services and infrastructure, and enterprise architecture support. To accomplish this, the E-Authentication Team, plans to build and operate a web-based E-Authentication Gateway. The

Gateway will provide common authentication services and single sign-on capability for all E-government services. The objective is to provide a set of common, shared services that all Federal agencies can use for authenticating the public.



PMC E-Gov Strategy

Government to Citizen	Managing Partner
1. USA Service	GSA
2. EZ Tax Filing	Treasury
3. Online Access for Loans	DoEd
4. Recreation One Stop	DOI
5. GovBenefits	Labor

Government to Business	Managing Partner
1. Federal Asset Sales	GSA
2. Online Rulemaking Management	DOT
3. Simplified and Unified Tax and Wage Reporting	Treasury
4. Consolidated Health Informatics	HHS
5. Business Compliance 1 Stop	SBA
6. Int'l Trade Process Streamlining	DOC

Cross-cutting: E-Authentication GSA, Enterprise Architecture OMB

Government to Government	Managing Partner
1. e-Vital	SSA
2. e-Grants	HHS
3. Disaster Assistance and Crisis Response	FEMA
4. Geospatial Information One Stop	DOI
5. SAFECOM	Treasury

Internal Effectiveness & Efficiency	Managi Partne
1. e-Training	OPM
2. Recruitment One Stop	OPM
3. Enterprise HR Integration	OPM
4. e-Travel	GSA
5. eClearance	OPM
6. ePayroll	OPM
7. Integrated Acquisition	GSA
8. e-Records Management	NARA

The e-Authentication Team is committed to implementing prototype Gateway authentication services beginning October 2002 with production authentication Gateway services targeted for September 2003. The production Gateway will be scaled to support all 24 initiatives as well as other E-Gov business needs for authentication across agencies.

Gateway Purpose and Scope:

Purpose: To provide common authentication services in support of Federal E-Government programs. The Gateway will provide single sign-on capability so that users of E-Government services do not have to meet multiple authentication and sign-on authentication requirements.

Scope: Initially the E-Authentication Gateway will be scaled as a prototype service. Agencies with applications approved by the Presidents Management Council as part of the Administration's E-Gov strategy (see chart on previous page) and, potentially, other agency E-Gov applications that are ready may be authorized to use the Gateway. Ultimately, all Federal agencies with E-Government processes requiring authentication will be able to use the Gateway.

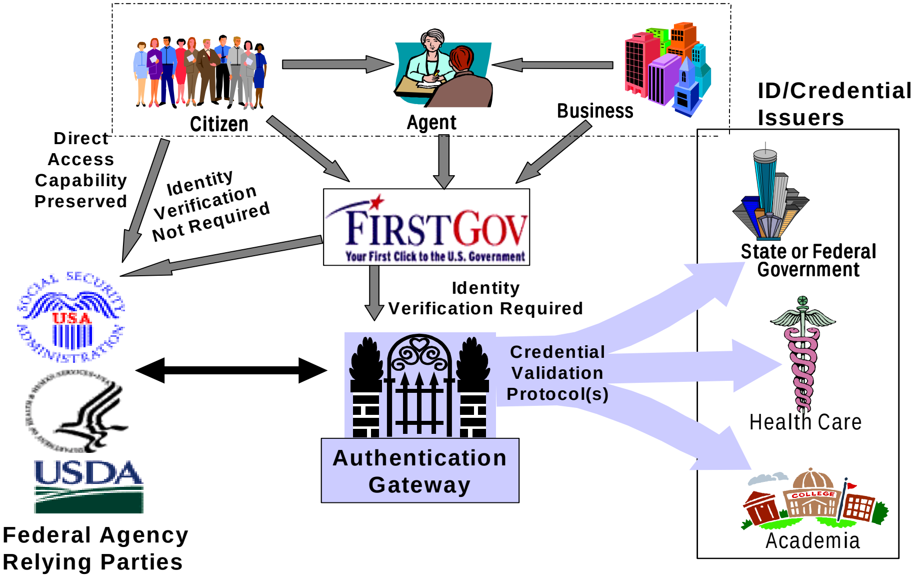
Types of Authentication accepted: The Gateway will be technology agnostic, in other words, it will accept multiple forms of authentication and differing credentials. This may require that the Gateway support multiple validation protocols to ensure the current validity and authenticity of credentials. It may also require the establishment of an organizational entity and process to determine the acceptability and trust of different forms of credentials. Currently, the Federal Government supports such an accrediting entity only for digital credentials issued using Public Key encryption technology (i.e., the Federal PKI Policy Authority)[1].

Users: The user population for the 24 E-Gov initiatives is very broad. Initially, the number of users and applications may be limited, at least until the full scalability of the Gateway is assured, but the ultimate scope of users will include all citizens, businesses and government agencies in the U.S. Use of the Gateway will be voluntary for the public.

Authorized uses: Initially, the only authorized uses of the Gateway will be to support the 24 Federal E-Gov initiatives and, potentially, other key E-Gov initiatives that are ready for such authentication services. Ultimately any Federal agency with E-Gov services requiring authentication will be able to use the Gateway. The Gateway is not contemplated for authentication services outside of the Federal Government. Use of the Gateway will be voluntary to Federal agencies.

[1] The United Kingdom helped establish TScheme to operate in this capacity.

The Authentication Gateway


Citizen
Agent
Business
ID/Credential Issuers
Direct Access Capability Preserved
Identity Verification Not Required
FIRSTGOV
Your First Click to the U.S. Government
Identity Verification Required
State or Federal Government
Credential Validation Protocol(s)
Health Care
Authentication Gateway
Academia
USDA
Federal Agency Relying Parties

Gateway Core Functionality:

The high-level schematic above presents the general context of the Gateway. The Gateway will be Internet-based and linked directly to FirstGov, the web-based portal to the Federal Government. As indicated by the schematic, the Gateway will be accessed through the FirstGov portal and through direct links with agency applications requiring authentication.

Following are core principles for the Gateway:

- Each level of information assurance has specific identity authentication requirements and may use a different authentication solution to determine trust.

- If an individual requires a higher information assurance level to transact business, they will be able to upgrade to the next assurance level.

- An identity assurance that allows access at a higher assurance level will be accepted by processes requiring lower assurance levels.

The e-Authentication team is currently developing requirements. The business model for using the Gateway has not yet been established. However, it is expected that agencies will enter into a Memorandum of Understanding (MOU) with GSA in order to clarify roles and responsibilities and authorize agency use of the Gateway.

Enrollment:

- Agencies with applications requiring authentication will enroll in the Gateway by executing an MOU with GSA.

- The enrolling agency will specify the level of authentication required for each application through the MOU.

- It is anticipated that GSA will maintain an authorization control system on behalf of the agency applications. The authorization control would ensure that authentication requirements meet the assurance levels specified for each Agency application. This system will be a logical, rules-based system for all applications supported by the Gateway.

Validation of Credentials:

- The Gateway will validate the authenticity of credentials. The Gateway may need to support multiple protocols for such validation. Public key certificates represent the only credential for which standardized processes for validation are in place today. The Federal Government may find it necessary to establish standard protocols for validating other forms of identity credentials.

- The Validation process will include querying the credential-issuing entity concerning the authenticity of the credential. This may require agreements between the Gateway operating authority and the credential issuers.

Agency Application Interface:

- The Gateway will support a standard interface(s) with agency applications.

- The gateway will support a standard protocol(s) for interfacing with agency applications. The protocol will include presenting the information concerning the authenticated user in a standard way for the agency applications to accept that information.

Legal and Policy Structures: GSA is authorized to provide goods and services to the entire Federal Government. Such services include information technologies and security services. The GSA has statutory authority to provide IT and E-Gov services, such as those contemplated for the E-Authentication initiative, to the Federal Government. Similarly, GSA established the Access Certificates for Electronic Services program (ACES) for PKI services and Common Access Card program for smart card services, under this statutory authority. These service offerings are available through government-wide contract awards. These contracts provide for the issuance of identity credentials to Federal employees and to the public. The legal structure for these services was established by GSA through legally binding contracts with third-party service providers. In addition, other agencies with more limited authorities have potentially suitable services for segments of users, which will be leveraged, to the extent possible. GSA intends to provide Gateway services through contract(s) with one or more third-party service providers.

The protection of privacy and private information is a primary policy objective for the Gateway and E-Authentication services. It is not contemplated that the E-Authentication Gateway would collect or maintain personal information. The Federal Government will ensure that the Gateway and the E-Authentication services are used only for their intended purposes as described above. The Gateway and other E-Gov services and infrastructure will comply with and support the Office of Management and Budget federal information privacy standards, requirements and guidelines for Electronic Government.

Next Steps:

The E-Authentication Team will proceed with building the policy and privacy framework (e.g., policies, practices, reviews, communications) for the Authentication Gateway that will lead to public confidence and trust in using Federal E-Gov services. Several key steps will be taken:

- Conduct risk assessments for all 24 E-Government initiatives to determine the appropriate levels of assurance and map to known classes of credentials.
- Map business processes and technical solutions to the data security, privacy, and protection requirements of the system of records and Gateway operations.
- Design, test and deploy the Gateway prototype beginning in September 2002.
- Conduct a full and open competitive bid process for the acquisition of a fully functional Gateway, whose requirements are based on the lessons learned from the prototype deployment.
- Evaluate and test the Production Gateway for large-scale deployment and rollout in September 2003.
- Determine the need for and develop, as appropriate, branding and marketing for the Authentication Gateway and/or the Presidents Management Council E-Government strategy in order to further build trust and protect the Government's e-Gov services.